REMARKS/ARGUMENTS

Specification

Pages 1 and 2 of the specification have been amended to update the list of co-pending applications with USPTO application and granted serial numbers.

Claim Rejections – 35 USC §103

Claims 1-5 and 7-17 were rejected under 35 U.S.C. 102(e) as being unpatentable over Eldridge et al. (U.S. Patent No. 6,515,988) in view of Stefik (U.S. Patet No. 5,715,403). The rejection is respectfully traversed.

The Examiner acknowledged that "Eldridge does not disclose obtaining authentication information at a printer." However, the Examiner states that Stefik discloses, at col. 3, lines 34-50, both a) receiving, at the printer and at the first server, an authorization identifier requrest requesting the allocation of an authorization identifier; and c) providing to a user, at the printer, the authorization identifier and the printer identifier. The Applicants respectfully disagree.

Stefik, at col. 3, lines 34-50, merely summarizes US. Pat. No. 5,247,575 to Sprague et al. Sprague et al. discloses an information distribution system that provides encrypted information packages (IPs) at a user site. The IPs may include journal articles, legal references, etc. See Sprague et al. at col. 15, lines 48-51. Keys for decrypting the IPs are installed in a user apparatus that decrypts specific IPs selected by a user on a pay-per-package basis. See Sprague et al. at col. 16, lines 39-58. Neither Sprague et al. nor Stefik disclose or fairly suggest providing to a user at a printer an authorization identifier and a printer identifier.

Furthermore, Stefik and Sprague et al. do not even appear to be concerned with the control of access to printers. And, *a fortiori*, these references do not disclose control of access to a printer through a method that first requires proof of physical access to the printer. As argued previously, a key concept behind the present invention—and a key limitation of the present claims that has still not been acknowledged by the Examiner—is that the present method enables secure access to printers by requiring a printer authorization identifier to be physically obtained at the printer itself. The method of the present invention guarantees that a later user of the printer, who accesses the printer from a web terminal, must have had some form of physical access to the printer in order to obtain the secret authorization identifier—which was provided only at the printer.

The method of the present claims is thus very useful for minimizing, for example, printer spamming when a printer is accessible through the Internet. For instance, a home or business user of the present invention, who has both a local printer and a local personal computer (PC), may desire to print to the printer from the PC via the internet, i.e., without a direct connection between the PC and the printer. The method of the present invention enables such a home or business user to print an authorization identifier at the local printer and then use that identifier to gain access to the printer through the Internet. It is envisioned that physical access to the printer could be obtained by, for example, receiving a physical page printed at the printer, where the page includes the authorization identifier. Alternatively the printer could provide the authorization identifier on a display screen on the printer, or in any other manner that is understandable to a user that is in the physical vicinity of the printer.

As argued above, the Applicants respectfully submit that the new art cited by the Examiner does not disclose, alone or in view of other cited art, the limitations of the present claims. Accordingly, it is submitted that the application is now in condition for allowance. Reconsideration and allowance of the application is courteously solicited.

Very respectfully,

Applicant: Paul Lapstun

PAUL LAPSTUN

KIA SILVERBROOK

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com
Telephone: +612 9818 6633
Facsimile: +61 2 9555 7762